# Algebra: The Basics of It

Adair Antonio da Silva Neto

November 25, 2021

# Contents

# 1 Introduction

In this text, we'll assume just basic Set Theory, involving the concepts of relations, equivalence classes, Cartesian product and so on.

So... what is algebra about?

# 2 Definitions

## 2.1 Ring

Think about the set of integers $\mathbb{Z}$ and the operations $+$ and $\times$ on it. What properties do these operations satisfy?

We know that addition is associative and commutative and that it has a neutral element denoted by $0$ and an inverse element.

With respect to multiplication, it is associative and commutative, it has a neutral element and the addition is distributive with respect to multiplication.

A ring is a generalization of these properties that we already know. In this section, we are going to study sets with two operations $+$ and $\times$ that satisfy the properties elucidated above. These operations are not necessarily the addition and multiplication that we know for $\mathbb{Z}$.

**Definition 2.1** (Ring)**.** A **commutative ring** $(A, +, \times)$ is a set $A$ with at least two elements, an operation denoted by $+$ (called addition) and an operation denoted by $\times$ (called multiplication) satisfying:

A1) Addition is **associative**: $\forall x, y, z \in A, (x + y) + z = x + (y + z)$

A2) Addition has a **neutral element**: $\exists 0 \in A$ such that $\forall x \in A, 0 + x = x$ and $x + 0 = x$.

A3) Addition has an **inverse element**: $\forall x \in A, \exists z \in A$ such that $x + z = 0$ and $z + x = 0$.

A4) Addition is **commutative**: $\forall x, y \in A, x + y = y + x$.

M1) Multiplication is **associative**: $\forall x, y, z \in A, (x \times y) \times z = x \times (y \times z)$.

M2) Multiplication has a **neutral element**: $\exists 1 \in A$ such that $\forall x \in A, 1 \times x = x$ and $x \times 1 = x$. $1$ is also called **identity**.

M3) Multiplication is **commutative**: $\forall x, y \in A, x \times y = y \times x$.

D) Addition is **distributive** with respect to multiplication: $\forall x, y, z \in A, x \times (y + z) = x \times y + x \times z$.

We may denote $a \times b$ by $a \cdot b$ or simply $ab$ and context will elucidate.

If, for a given ring, all these properties are satisfied except for the commutative of multiplication, then we'll call it a non-commutative ring.

Some important remarks:

- The neutral element is unique, both for addition and multiplication.
- The inverse element, with respect to addition, is unique.
- The neutral element of addition has the following property: $0 \cdot x = 0, \forall x \in A$.

We also define a **subring** of a ring as the subset which is closed under the operations of addition, subtraction, and multiplication and also contains the element $1$.

Before heading to some examples, let give two important definitions.

## 2.2 Domain

If the product of any two non-zero elements of a given ring $D$ is different than zero, then this ring is called a **domain** or an **integral domain**.

$$\text{M4)}\ \forall x, y \in D \setminus \{0\},\ x \times y \neq 0$$

Hence, if $D$ is an integral domain, $a, b, c \in D$ and $ab = ac$, then $a \neq 0$ implies $b = c$. This is called **cancellation law**.

An immediate example of a domain is $(\mathbb{Z}, +, \times)$.

## 2.3 Field

If every non-zero element of a given ring has a multiplicative inverse, then this ring is called a **field**. Symbolically,

$$\text{M4')}\ \forall x \in K \setminus \{0\},\ \exists y \in K : x \times y = 1$$

This inverse is also unique and the inverse of $x$ is denoted by $x^{-1}$.

Please take notice that this property is stronger than the property that defines a domain. That means that is $K$ is a field, then $K$ is also a domain. Although not all domains are fields, if the domain has a finite number of elements, then it is a field.

E.g. $(\mathbb{Q}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times)$ are fields.

# 3 Examples

## 3.1 Gaussian Integers

Let $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$. Then $(\mathbb{Z}[i], +, \times)$ is a domain called **Gaussian integers**. This idea can be generalized by defining a subring generated by $n$ as $\mathbb{Z}[n]$.

## 3.2 Direct product

Given two rings $(A_1, +_1, \cdot_1)$ and $(A_2, +_2, \cdot_2)$, it's possible to construct a new ring defining:

- The set $A_1 \times A_2 := \{(a_1, a_2) \,|\, a_1 \in A_1, a_2 \in A_2\}$
- Addition: $(a_1, a_2) + (a_1', a_2') := (a_1 +_1 a_1', a_2 +_2 a_2')$
- Multiplication: $(a_1, a_2) \times (a_1', a_2') := (a_1 \cdot_1 a_1', a_2 \cdot_2 a_2')$.

Then $(A_1 \times A_2, +, \cdot)$ is a ring called **direct product** of $A_1$ and $A_2$.

## 3.3 Ring of integers modulo n

Let $n \in \mathbb{Z}_+$ and define the relation $\underset{n}{\equiv}$ as: given $a, b \in \mathbb{Z}$,

$$a \underset{n}{\equiv} b \iff a - b \text{ is a multiple of } n$$

And we say that $a$ is congruent to $b$ modulo $n$. Notice that $\underset{n}{\equiv}$ is an equivalence class.

The equivalence class of $a$ is denoted by $\bar{a} = \{b \in \mathbb{Z} \,|\, b \underset{n}{\equiv} a\} = \{a + kn, k \in \mathbb{Z}\}$.

We also write $\mathbb{Z}/n\mathbb{Z}$ to denote the set of equivalence classes modulo $n$, i.e. $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$. And we define the following compositions over it:

$$\begin{aligned} \underset{n}{\oplus} : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ (\bar{x}, \bar{y}) &\mapsto \overline{x+y} \\ \underset{n}{\odot} : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ (\bar{x}, \bar{y}) &\mapsto \overline{xy} \end{aligned}$$

Then $(\mathbb{Z}/n\mathbb{Z}, \underset{n}{\oplus}, \underset{n}{\odot})$ is a ring, where the neutral element for $\underset{n}{\oplus}$ is the class $\bar{0}$, the neutral element for $\underset{n}{\odot}$ is $\bar{1}$, and the inverse of $\bar{x}$ with respect to $\underset{n}{\oplus}$ is the class $\overline{-x}$.

Notice that if $p$ is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ is a field.

## 3.4 Ideal

Before going to next example, a simple definition is necessary.

**Definition 3.1** (Ideal)**.** If $I \subseteq A$, $I \neq \emptyset$, then $I$ is called an **ideal** of $A$ if

- $x + y \in I, \forall x, y \in I$.
- $ax \in I, \forall x \in I, \forall a \in A$.

This definition is equivalent to saying that, given $I$ non empty, a linear combination $a_1x_1 + \ldots a_rx_r$ of elements $x_i \in I$ with coefficients $a_i \in A$ is in $I$.

For example, $n\mathbb{Z} := \{zn \,|\, z \in \mathbb{Z}\}$ is an ideal of the ring of integers (where $n$ is a non-negative integer).

In any ring $A$, the set of multiples of a particular element $a$ (i.e. the set of elements divisible by $a$) forms an ideal called **principal ideal**. Symbolically, this ideal is the set $\{ax : a \in A\}$.

It's also useful to define the **ideal generated by** a set of elements $a_1, \ldots, a_n \in A$, which is the smallest ideal containing the elements. A ring in which every ideal if finitely generated is called **Noetherian ring**.

This concept allows us to make constructions analogous to the ring of integers modulo $n$. In general, an ideal is not a ring because it usually lacks the element $1$.

## 3.5 Quotient ring modulo an ideal

Given a ring $A$ and $I$ an ideal of $A$, define the following congruence relation: for $a, b \in A$,

$$a \equiv b \mod I \iff a - b \in I$$

Which is also an equivalence relation.

If $a \in A$, then its class of equivalence modulo $I$ is given by $\bar{a} := \{b \in A \,|\, b \equiv a \mod I\} = \{a + c \,|\, c \in I\}$. We denote $A/I$ the set of equivalence classes modulo $I$, and we define the following operations over it: for $\bar{x}, \bar{y} \in A/I$,

$$\bar{x} \underset{I}{\oplus} \bar{y} := \overline{x + y} \text{ and } \bar{x} \underset{I}{\odot} \bar{y} := \overline{x \cdot y}$$

These operations are well defined and $(A/I, \underset{I}{\oplus}, \underset{I}{\odot})$ is a ring called **quotient ring modulo an ideal**.

# 4 Polynomial Rings

**Definition 4.1** (Polynomial Ring)**.** A polynomial with coefficients in any ring $R$ is a linear combination of the powers of the variable:

$$f(x) = a_0 + a_1 x + ldots + a_{n-1}x^{n-1} + a_n x^n$$

where $a_0, a_1, \ldots, a_{n-1}, a_n \in R$. This is called a **polynomial in one variable over R** and is written $R[x]$. In fact, $R[x]$ is a ring, with the sum and product

defined as follows.

Let $g(x) = b_0 + b_1x + b_2x^2 + \ldots$ be a polynomial in the same ring. Then the sum of $f$ and $g$ is

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots = \sum_k (a_k + b_k)x^k$$

which corresponds to the vector addition. And the product is computed by multiplying term by term and collecting coefficients of the same degree in $x$. Expanding the product, we obtain

$$f(x)g(x) = \sum_{i,j} a_i b_j x^{i+j} = p_0 + p_1x + p_2x^2 + \ldots$$

where $p_k = a_0b_k + a_1b_{k-1} + \ldots + a_kb_0 = \sum_{i+j=k} a_ib_j$.

Some important definitions:

1. The **degree** $n$ of $f(x)$ is the largest power of $a_i$ such that $a_i \neq 0$.
2. If $n$ is the degree of the polynomial, then $a_n$ is called **leading coefficient**.
3. If $a_n = 1$, then $f(x)$ is called **monic**.

**Example 4.1.** Let $R$ be a ring, $f(X), g(X) \in R[X] \setminus \{0\}$. Show that:

1. If $R$ is a domain, then
$$\deg(f(X) \cdot g(X)) = \deg f(X) + \deg g(X)$$
2. $R[X]$ is a domain iff. $R$ is an integral domain.

*Proof.* Suppose that $R$ is a domain and consider two polynomials $f$ and $g$ over it. Let $m$ be the degree of $f$ and $n$, the degree of $g$. Also letting $a_m$ be the leading coefficient of $f$ and $b_n$, the leading coefficient of $g$, the leading term of $fg = a_mb_nx^{m+n}$. Since $a_mb_n \neq 0$ (because $R$ is a domain), the degree of $f \cdot g$ is $m + n$ which is exactly what we needed for the first item.

($\Leftarrow$) Suppose that $R$ is a domain with both $f, g \neq 0$. Then $\deg(f(X) \cdot g(X)) = \deg f(X) + \deg g(X)$ implies that $a_mb_n \neq 0$. Hence, $R[X]$ is a domain.

($\Rightarrow$) Suppose that $R[X]$ is a domain. Then for $f, g \neq 0$, $fg \neq 0$. Therefore, its leading term $a_m b_n \neq 0$. Which means that any pair of non-negative elements of $R$ is different than zero, i.e., $R$ is a domain. ■

**Definition 4.2** (Ring of polynomials in $k$ variables)**.** By induction, we can define the **ring of polynomials in $k$ variables** as follows:

$$A[X_1, \ldots, X_k] = A([X_1, \ldots, X_{k-1}])[X_k]$$

For k=2 we have $A[X_1, X_2] = (A[X_1])[X_2]$:

$$\begin{aligned} f(x_1, x_2) &= a_{nm} x_1^n x_2^m + \ldots + a_{11} x_1 x_2 + a_{10} x_1 + a_{01} x_2 + a_{00} \\ &= \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} x_1^i x_2^j \end{aligned}$$

**Definition 4.3** (Associated polynomial function)**.** GGiven $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$, we can define the **associated polynomial function** $\bar{f} : A \to A$ defined by $\bar{f}(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$.

Please take notice that the polynomial function $\bar{f}$ and the **formal polynomial** $f$ are different things.

# 5 Euclidean Domains

The Euclidean Algorithm shows that in $\mathbb{Z}$ we can divide an element $a$ by another element $b$ obtaining a remainder such that its absolute value is smaller then the absolute value of $b$.

To generalize that idea, we need a set with addition and multiplication and some way to measure if an element of the set is smaller than the other. Intuitively, an euclidean domain is an integral domain in which there is an algorithm similar to that of Euclid.

**Definition 5.1** (Euclidean Domain)**.** An **euclidean domain** $(D, +, \cdot, \varphi)$ is an integral domain $(D, +, \cdot)$ with a function

$$\varphi : D \setminus \{0\} \to \mathbb{N}$$

satisfying:

1. $\forall a, b \in D, b \neq 0$ there are $t, r \in D$ such that $a = bt + r$ where $\varphi(r) < \varphi(b)$ or $r = 0$.
2. $\varphi(a) \leq \varphi(ab)$, $\forall a, b, \in D \setminus \{0\}$.

**Theorem 5.1** (Euclid Algorithm for $\mathbb{Z}$). *Let $|\cdot| : \mathbb{Z} \to \mathbb{N}$ the absolute value function. Then:*

1. $(\mathbb{Z}, +, \cdot, |\cdot|)$ *is an euclidean domain, i.e.*
   - $(\mathbb{Z}, +\cdot)$ *is a domain.*
   - $\forall a, b \in \mathbb{Z}, b \neq 0$ *there are* $t, r \in \mathbb{Z}$ *such that* $a = bt + r$ *where* $|r| < |b|$ *or* $r = 0$.
   - $|a| \leq |ab|$, $\forall a, b, \in \mathbb{Z} \setminus \{0\}$.
2. $t$ *and* $r$ *can be computed.*
3. *In general,* $t$ *and* $r$ *are not unique.*
4. *It's always possible to choose* $r \geq 0$ *in a unique way.*

Using this theorem, we can find that all ideals of $(\mathbb{Z}, +, \cdot)$ are of the form $n\mathbb{Z}$ with $n \geq 0$.

**Definition 5.2** (Norm). The function

$$\begin{aligned} N : \mathbb{C} &\to \mathbb{R} \\ a + bi &\mapsto (a + bi)(a - bi) \end{aligned}$$

is called **norm**.

**Theorem 5.2** (Gaussian Integers). *Let $\mathbb{Z}[i]$ the ring of Gaussian integers and $N : \mathbb{Z}[i] \to \mathbb{N}, N(a + bi) = a^2 + b^2$ the norm function. Then*

1. $(\mathbb{Z}[i], +, \cdot, N)$ *is an euclidean domain.*
2. $t$ *and* $r$ *can be computed.*
3. *In general,* $t$ *and* $r$ *are not unique.*

An example of euclidean domain with polynomial rings is the **division of polynomials**.

Given a ring $R$, $f(x), g(x) \in R[x]$, where the leading coefficient of $g(x)$ is invertible in $R$, then the following affirmations hold:

1. There are $t(x), r(x) \in R[x]$ such that $f(x) = g(x)t(x) + r(x)$ where $\deg r(x) < \deg g(x)$ or $r(x) = 0$.

2. The polynomials $t(x)$ and $r(x)$ can be effectively computed.

3. The polynomials $t(x)$ and $r(x)$ are uniquely determined.

**Example 5.1.** Let $(T, +, \cdot)$ be a ring and $R \subseteq T$ a subset such that $(R, +, \cdot)$ is a ring. Also let $f(x), g(x) \in R[x]$ where the leading coefficient of $g(x)$ is invertible in $R$.

Show that if $t(x), r(x) \in T[x]$ satisfies

$$f(x) = g(x)t(x) + r(x) \text{ with } \deg r(x) < \deg g(x) \text{ or } r(x) = 0$$

then $t(x), r(x) \in R[x]$.

*Proof.* If $f(x) = 0$ or $\deg f(x) < \deg g(x)$ then $t(x) = 0$ and $r(x) = f(x)$. Since $R$ is a ring, then $0 \in R$, i.e. $t(x), r(x) \in R[x]$.

If $\deg f(x) \geq \deg g(x) = m$, then let $f(x) = a_n x^n + \ldots + a_0$, where $n \geq m$ and $a_n \neq 0$. And write $g(x) = b_m x^m + \ldots + b_0$. Since $b_m$ is invertible, $\frac{1}{b_m} \in R$ and it's possible to apply the polynomial division obtaining a remainder and a quotient which are both computed using the coefficients of $f$ and $g$. Hence, $t(x), r(x) \in R[x]$ as desired. ■

# 6 Ring Homomorphisms

Intuitively, a ring homomorphism is a function between rings preserving both operations and the identity element. We can define it rigorously as follows.

**Definition 6.1** (Ring Homomorphisms)**.** Let $(A, +, \cdot)$ and $(B, \oplus, \odot)$ two rings. A map $f : A \to B$ is called an **homomorphism** if, for all $x, y \in A$,

1. $f(x + y) = f(x) \oplus f(y)$

2. $f(x \cdot y) = f(x) \odot f(y)$

3. $f(1_A) = 1_B$

Before heading on, let us consider some examples of homomorphisms:

**Identity**: $Id : A \to A$ where $a \mapsto a, \forall a \in A$.

Given $I$ is an ideal of the ring $A$, an application $\varphi : A \to A/I$, where $\varphi(a) = a + I$, is an homomorphism called **canonical homomorphism** (or canonical projection).

$\varphi : (\mathbb{Z}, +, \cdot) \to (B, \oplus, \odot)$ is defined as

$$\varphi(n) = 1_B \oplus 1_B \oplus \ldots \oplus 1_B \text{ n times}$$
$$\varphi(-n) = (-1_B) \oplus (-1_B) \oplus \ldots \oplus (-1_B) \text{ n times } \forall n \geq 0$$

is an homomorphism. In fact, it is the **only homomorphism** from $\mathbb{Z}$ to $B$.

If $A_1, \ldots, A_r$ are rings and $(A_1 \times \ldots \times A_r)$ is a direct product, then, for $i$ ranging from $1$ up to $r$

$$p_i : A_1 \times \ldots \times A_r \to A_i$$
$$(a_1, \ldots, a_r) \mapsto a_i$$

is an homomorphism called **i-th projection**.

If $f : A_1 \to A_2$ and $g : A_2 \to A_3$ are homomorphisms, then the **composition** $g \circ f : A_1 \to A_3$ is a homomorphism.

**Theorem 6.1** (Substitution Principle)**.** *Let $\varphi : R \to R'$ be a ring homomorphism.*

- *Given an element $a \in R'$, there is a unique homomorphism $\Phi : R[X] \to R'$ which agrees with the map $\varphi$ on constant polynomials and sends $x \mapsto a$.*
- *More generally, given $a_1, \ldots, a_n \in R'$, there is a unique homomorphism $\Phi : R[x_1, \ldots, x_n] \to R'$ which agrees with $\varphi$ on constant polynomials and send $x_i \mapsto a_i$ for $i = 1, \ldots, n$.*

Intuitively, the substitution principle says that $\Phi$ acts on the coefficients of the polynomial exactly like $\varphi$ and substitutes $a$ for $x$.

## 6.1 Elementary properties

Consider $f : (A, \underset{A}{+}, \underset{A}{\cdot}) \to (B, \underset{B}{+}, \underset{B}{\cdot})$ a ring homomorphism.

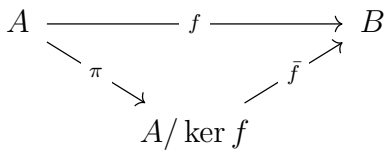
1. Let $\ker f := \{a \in A : f(a) = 0\} \subseteq A$. Then $\ker f$ is an ideal of $A$ called **kernel** of $f$.
2. Let $\mathrm{Im} f := \{f(a) : a \in A\} \subseteq B$. Then $(\mathrm{Im} f, \underset{B}{+}, \underset{B}{\cdot})$ is a ring called **range** of $f$.
3. $f$ is injective (i.e. one-to-one) iff. $\ker f = \{0\}$.
4. $f$ is called **isomorphism** if $f$ is both injective and surjective. In this case, there is an inverse map $f^{-1} : B \to A$ which is also a ring homomorphism. And we say that $A$ and $B$ are isomorphic.

## 6.2 The Isomorphisms Theorem

**Theorem 6.2** (The Isomorphisms Theorem)**.** *Consider a ring homomorphism $f : (A, +, \cdot) \to (B, \oplus, \odot)$. Then the mapping $\bar{f}$ defined as*

$$\begin{aligned} \bar{f} = (A/\ker f, \underset{\ker f}{\oplus}, \underset{\ker f}{\odot}) &\to (\mathrm{Im} f, \oplus, \odot) \\ \bar{a} &\mapsto f(a) \end{aligned}$$

*is a ring isomorphism, which can be visualized by the following diagram:*




**Theorem 6.3** (Chinese Remainder Theorem)**.** *Let $m_1, \ldots, m_r$ positive integers, where each pair is relatively prime. Then the diagonal application*

$$\begin{aligned} \Delta : \mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z} \\ z &\mapsto (z + m_1\mathbb{Z}, \ldots, z + m_r\mathbb{Z}) \end{aligned}$$

*is surjective. This is equivalent to $\forall z_1, \ldots, z_r \in \mathbb{Z}, \exists z \in \mathbb{Z}$ such that*

$$\begin{aligned} z &\equiv z_1 \mod m_1 \\ z &\equiv z_2 \mod m_2 \\ &\vdots \\ z &\equiv z_r \mod m_r \end{aligned}$$

Generalizing this result, we obtain the following

**Theorem 6.4.** *Let $m_1, \ldots, m_r$ positive integers, where each pair is relatively prime. Then the application*

$$\begin{aligned} \bar{\Delta} : \mathbb{Z}/m_1 \ldots m_r\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z} \\ z + m_1 \ldots m_r\mathbb{Z} &\mapsto (z + m_1\mathbb{Z}, \ldots, z + m_r\mathbb{Z}) \end{aligned}$$

*is a ring isomorphism.*

**Definition 6.2** (Characteristic of a Ring)**.** Consider $R$ a ring and $\varphi : \mathbb{Z} \to R$ the only homomorphism from $\mathbb{Z}$ to $R$. Since $\ker \varphi$ is an ideal of $\mathbb{Z}$, there is a unique integer $c \geq 0$ such that $\ker \varphi = c\mathbb{Z}$. This integer $c$ is called **characteristic** of the ring $R$.

That means that $c$ generates the kernel of the homomorphism $\varphi$. I.e., $c$ is the smallest positive integer such that $c$ times $1_R = 0$. If $\ker = \{0\}$, the characteristic is zero. For example, $\mathbb{R}, \mathbb{C}$ and $\mathbb{Z}$ have characteristic zero.

# 7 Factorization

**Definition 7.1** (Factor)**.** Let $R$ an ring and $a \in R$. An element $b \in R$ is called a **divisor** or **factor** of $a$ in $R$ if there is $c \in R$ such that $a = bc$. We also say that $b$ divides $a$ and that $a$ is a multiple of $b$. We denote $b|a$.

**Definition 7.2** (Invertible)**.** An element $a \in R$ is **invertible** in $R$ if there is $b \in R$ such that $ab = 1$. We denote $R^*$ the set of invertible elements.

**Definition 7.3** (Associated)**.** Two elements $a, b \in R$ are **associated** in $R$ if there is $u \in R$, $u$ invertible, such that $a = ub$.

**Definition 7.4** (Irreducible)**.** A non-invertible $a \in R \setminus \{0\}$ is **irreducible** in $R$ if $a$ only has a trivial factorization in $R$, i.e.,

$$\forall b, c \in R \text{ such that } a = bc \implies b \text{ or } c \text{ is invertible in } R$$

**Definition 7.5** (Prime)**.** A non-invertible $p \in R$ is **prime** if

$$\forall a, b \in R,\ p|ab \implies p|a \vee p|b$$

**Definition 7.6** (Greatest Common Divisor)**.** Let $a_1, \ldots, a_n \in R$. An element $d \in R$ is called **Greatest Common Divisor** of $a_1, \ldots, a_n$ if $d$ divides $a_1, \ldots, a_n$ and if every $d' \in R$ that divides $a_1, \ldots, a_n$ also divides $d$. The elements $a_1, \ldots, a_n$ are called **relatively prime** if their GCD is equal to one.

In an integral domain, two GCDs for $a_1, \ldots, a_n$ are associated. Hence, the GCD is unique (up to multiplication for invertible elements) in a domain. This is not generally valid for a ring.

Consider an euclidean domain $(D, \varphi)$. Then

$$\varphi(b) = \varphi(ba) \text{ if } a \text{ is invertible,}$$

$$\varphi(b) < \varphi(ba) \text{ if } a \text{ is not invertible.}$$

If $D$ is not a field, then let

$$\begin{aligned}\delta &= \min\{\varphi(d) | d \in D, d \text{ non-invertible}\} \\ &= \min\{\varphi(d) | d \in D, d\varphi(d) > \varphi(1)\}\end{aligned}$$

Then $\{a \in D | \varphi(a) = \delta\} \subseteq \{a \in D | a \text{ is irreducible }\}$.

**Definition 7.7** (Unique factoring domain)**.** A domain $D$ is a **unique factoring domain** or **factorial domain** if every non-zero and non-invertible element of $D$ can be written uniquely as the product of irreducible elements of $D$. I.e.,

1. Every non-zero and non-invertible element of $D$ is a finite product of irreducible factors.
2. If $\{p_i\}_{1 \leq i \leq s}$ and $\{q_j\}_{1 \leq j \leq t}$ are finite families of irreducible elements of $D$ such that $p_1 \ldots p_s = q_1 \ldots q_t$ then
   - s = t
   - Up to ordering, $p_i$ is associated to $q_i, \forall i = 1, \ldots s$. That means that there is a bijective map $\sigma$ from $\{1, \ldots, s\}$ to $\{1, \ldots, s\}$ such that $p_i$ is associated to $q_{\sigma(i)}$.

**Theorem 7.1.** *Let $D$ a domain. Then the following are equivalent:*

1. *$D$ is factorial (satisfies both conditions of the definition above).*
2. *$D$ satisfies the first condition of the definition above and for all $p \in D$ irreducible and for all $a, b \in D$, $p|ab \implies p|a \vee p|b$.*

We can relate the GCD of some elements and the ideal generated by those elements.

## 7.1 Noetherian Domains

An ascending chain of ideals of a ring

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots$$

is **stationary** if there is $n \in \mathbb{N}$ such that $I_k = I_n$ for $k \geq n$.

Notice that if $D$ is a principal domain, then $D$ is a Noetherian domain.

**Theorem 7.2.** *Let $R$ be a ring. Then*

1. *$R$ is Noetherian iff. every ascending chain of ideals of $R$ is stationary.*
2. *If $R$ is a Noetherian domain, then every non-invertible element of $R \setminus \{0\}$ can be written as the finite product of irreducible elements.*
3. *$R$ is a principal domain iff. $R$ is a factorial domain where*

$$\forall a, b \in R \setminus \{0\}, \exists e, f \in R \text{ such that } \gcd\{a, b\} = ea + fb$$

**Theorem 7.3.** *Let $(D, \varphi)$ an Euclidean Domain. Then*

1. *$D$ is a principal domain.*
2. *$\forall a, b \in D \setminus \{0\}$ it's effectively computed $e, f \in D$ such that $\gcd\{a, b\} = ea + fb$ if the division in $D$ is effective.*

**Corollary 7.4.** *Consider $K$ a field and $f_1(X), f_2(X) \in K[X]$ two polynomials relatively prime. Let $k(X) \in K[X]$. Then:*

1. *It's possible to effectively compute $g_1(X), g_2(X) \in K[X]$ such that $k(X) = g_1(X)f_1(X) + g_2(X)f_2(X)$.*
2. *If $\deg k(X) < \deg f_1(X) + \deg f_2(X)$ then $g_1(X)$ and $g_2(X)$ can be taken satisfying*
   - *$\deg g_1(X) < \deg f_2(X)$ (or $g_1(X) = 0$).*
   - *$\deg g_2(X) < \deg f_1(X)$ (or $g_2(X) = 0$).*

Now we can generalize the Chinese Remainder Theorem for any principal domain.

**Theorem 7.5** (Chinese Remainder Theorem)**.** *Let $D$ a principal domain and $d_1, d_2, \ldots, d_r$ elements of $D$ where each pair is relatively prime. Then the map*

$$\begin{aligned} \bar{\Delta} : D \setminus (d_1 \ldots d_r) &\to (D \setminus (d_1)) \times \ldots \times (D \setminus (d_r)) \\ z + (d_1 \ldots d_r) &\mapsto (z + (d_1), \ldots, z + (d_r)) \end{aligned}$$

*is a ring isomorphism.*

# References


[Art91] Michael Artin. *Algebra*. Prentice-Hall, 1991.

[GL06] Arnaldo Garcia and Yves Lequain. *Elementos de álgebra*. Instituto de Matemática Pura e Aplicada, 2006.

[Lee18] Gregory T Lee. *Abstract algebra: An introductory course*. Springer, 2018.